Opinnäytetyö (AMK)

Tietojenkäsittely

Tietojärjestelmät

2014

Petteri Kivelä

TIETOTURVALLISUUDEN HALLINTAJÄRJESTELMÄN MITTAAMISEN KARTOITUS

TURUN AMMATTIKORKEAKOULU
TURKU UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ (AMK) | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Tietojenkäsittely | Tietojärjestelmät

2014 | 47 sivua

Esko Vainikka

Petteri Kivelä

TIETOTURVALLISUUDEN HALLINTAJÄRJESTELMÄN MITTAAMISEN KARTOITUS

Julkisyhteisöillä ja yrityksillä on käytössään erilaisia keinoja tietoturvallisuuden takaamiseksi. Järjestelmäksi muokattuna näitä kutsutaan tietoturvallisuuden hallintajärjestelmiksi. Hallintajärjestelmät eivät kuitenkaan ehkäise tietoturvauhkia, mikäli niitä ei käytetä oikein ja mikäli järjestelmiä seuraamassa ei ole ammattitaitoisia ja kyseiseen järjestelmään perehtyneitä henkilöitä. Opinnäytetyössä käytetään konstruktiivista tutkimusotetta, joka toteutuu tietoturvallisuuden avainhenkilöiden haastatteluiden kautta.

Tietoturvallisuuden hallintajärjestelmiä mittaamaan on kehitetty erilaisia tapoja ja mittaristoja. Tässä työssä käydään läpi miksi mittaamista tehdään, miten sitä tulisi tehdä ja mitä hyötyä tietoturvallisuuden mittaamisella on organisaatiolle. Tarkoituksena on esitellä sopiva mittaristo, joka vie vähän resursseja, mutta silti toimii tietoturvallisuuden hallintajärjestelmän toiminnan tarkistamisessa ja parantamisessa.

Työssä tarkastellaan pääasiassa ISO/IEC 27004-standardiin perustuvia tapoja mitata ISO/IEC 27001 -standardiin perustuvaa tietoturvallisuuden hallintajärjestelmää.

Tietoturvallisuuden avainhenkilöiden haastatteluista käy ilmi, että mittaristosta halutaan kevyt helposti käyttöönotettava portaittainen mittaristo. Työn tuloksena esitetään toteutettavaksi kuuden mittarin mittaristoa. Mittaristo on suppea syystä, jotta se saadaan osaksi liiketoimintaa ja hallintajärjestelmän kehittämistä. Mittariston paikaksi esitetään ServiceDeskiä.

Haastattelujen perusteella havaittiin tietoturvallisuuden mittaamisstandardin mukaisen mittariston sopimattomaksi. Valtiovarainministeriön tietoturvatasojen- ja ICT-varautumishankkeiden mittaamisosio on salainen. Työssä käytettiin näistä esitutkimushanketta, josta puuttuu mittaamisosio.

Työn loppupäätelmä on, että paras tapa luoda toimiva tietoturvallisuuden hallintajärjestelmän mittaristo on aloittaa muutamalla mitattavalla kohteella ja lisätä kohteita organisaation mittausten perusteella.

ASIASANAT:

Tietoturva, hallintajärjestelmä, ISO/IEC-standardi, mittaaminen

BACHELOR´S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Business Information Technology | Information Systems

2014 | 47 pages

Esko Vainikka

Petteri Kivelä

MEASUREMENT OF INFORMATION SECURITY MANAGEMENT SYSTEMS

Public and private corporations have different ways to manage their information security. Information security is managed through documenting where organization wants to go and by checking the day-to-day life to match that. These plans to better security, and the method to work to get there, are called information security management systems. These systems however don´t prevent security threats, if they are not correctly implemented and if an organization do not have competent personnel to monitor the systems.

Different ways of measurement and different kinds of instrumentations are developed to measure Information security management systems. This thesis covers different instrumentations, mainly based on ISO/IEC 27004 standard.

The interviews indicate that the measurement system should be sequential, lightweight and easy to deploy. The measurement system will include six meters.

The final conclusion is that the best way to create an effective measurement system for information security is to start with a limited set of the metrics and add metrics when measurements indicate that they are needed.

KEYWORDS:

Measurement, management systems, ISO/IEC-standard, information security

SISÄLTÖ

KUVIOT

TAULUKOT

KÄYTETYT LYHENTEET

ALE	Annual Loss Expectancy. Yksittäisen vahingon odotuksen vuotuinen esiintymistiheys.
BUQTRAQ	Tietoturvaongelmiin keskittynyt sähköpostituslista.
DNS	Internet-palvelu, joka muuntaa verkkotunnuksen IP-osoitteeksi.
FTP	File Transfer Protocol. Internettiä käyttävä tiedonsiirtomenetelmä.
ICT	Information and Communications Technology. Informaatio ja kommunikaatiotekniikka
IT	Information Technology. Informaatioteknologia.
PDCA	Plan-Do-Check-Act. Ongelmanratkaisumalli ja kehittämismenetelmä.
SEM	Security Event Management. Tietoturvaherätteidenhallinta.
SSH	Secure Shell. Salattuun tietoliikenteeseen tarkoitettu protokolla.
TCO	Total Cost of Ownership. Kehityksen ja ylläpidon kokonaiskustannukset.
WAN	Wide Area Network. Tiedonsiirtoverkko, joka peittää laajan maantieteellisen alueen.

1 JOHDANTO

Aloitin työharjoittelun julkishallinnossa keskushallinnon vastuualueen It-toiminnassa 11.1.2010. Työnkuvaani kuului tietoturvallisuuden auditointi liittyen ISO/IEC 27001 -standardiin sekä valtiovarainministeriön tietoturvatasot- ja ICT-varautuminen-hankkeisiin.

Harjoittelun tuloksena sain tehtäväkseni laatia kaupungin tietoturvallisuuden hallintajärjestelmään pohjautuvan opinnäytetyön. Tarkoituksena oli tutkia eri tapoja mitata tietoturvallisuutta. Alkuasetelma oli tarkastella kolmea tapaa mitata tietoturvallisuuden hallintajärjestelmää: ISO/IEC 27004:2009 Tietoturvallisuuden hallinta-standardin mukainen mittaaminen, Valtiovarainministeriön tietoturvatasoihin perustuva mittaaminen ja ICT-varautumiseen perustuva mittaaminen. Tässä työssä tarkastellaan ensisijaisesti mittaamisstandardiin ISO/IEC 27004 -perustuvia tapoja mitata ISO/IEC 27001 -standardiin perustuvaa tietoturvallisuuden hallintajärjestelmää.

Työssä käytetään huomattavan paljon lähteinä teoksia Hakkerin käsikirja (Anonymous, Balding & Kataja, 2002) ja IT Security Metrics (Hayden, 2010). Teosten julkaisuvuodesta huolimatta molempien sisältämät menetelmät ja periaatteet ovat edelleen päteviä, jos niitä käytetään yleisellä tasolla.

2 TIETOTURVAN TARVE

Laki velvoittaa julkisyhteisöjä, esimerkiksi kaupunkeja huolehtimaan tietoturvallisuudesta. Muun muassa Henkilötietolaki (22.4.1999/523) ja Laki yksityisyyden suojasta työelämässä (13.8.2004/759) asettavat velvoitteita erilaisten tietojärjestelmien ylläpitäjille.

Valtiovarainministeriössä toteutettu ICT-varautumisen esitutkimushanke on osoittanut kunnissa olevan monia puutteita häiriötilanteisiin varautumisessa. Ongelmia aiheuttavat mm. vanhentuneet tietojärjestelmät, palveluiden hankkiminen ulkoistamisen kautta, ICT-varautumiseen tarvittavien resurssien puute ja vanhentuneet varautumissuunnitelmat. Voidaan perustella, että ICT-järjestelmiin kohdistuva kriisitila aiheuttaa kuntien palveluille keskeytyksiä läpi kunnan palvelusektorin jo lyhyessä ajassa. (Valtiovarainministeriö 2011, 10.)

Tämä tarkoittaa sitä, että vanhentuneisiin tietojärjestelmiin ei välttämättä saa tietoturvapäivityksiä. Esimerkkinä on Windows XP-käyttöjärjestelmä, jonka tuki loppui 8.4.2014. Palveluiden ulkoistaminen aiheuttaa organisaation oman osaamisen katoamisen tai merkittävän vähenemisen. Resurssien puute taas kuormittaa tietoturvallisuuden työntekijöitä muilla töillä, jotka ovat aivan yhtä kiireisiä.

Konkreettisia haittoja ja vahinkoja, joita saattaa syntyä puutteellisesta tietoturvasta, ovat esimerkiksi luottamuksellisten tietojen ja asiakastietojen leviäminen, järjestelmien kaatuminen, erilaiset virheet sekä näiden johdannaisvaikutukset. Välilliset vahingot tietoturvaongelmista saattavat olla huomattavia. (Anonymous ym. 2002, 6.)

Tarkastellaan esimerkkiä sisäisestä uhasta. Suuryrityksellä on tyytymätön työn tekijä. Oletetaan, että hän päättää tehdä mahdollisimman paljon hallaa yrityksen toiminnalle. Tuhoa voidaan aiheuttaa esimerkiksi ohjelmoimalla yrityksen sisäiset järjestelmät suorittamaan automatisoituja ja hajautettuja palvelunestohyökkäyksiä avaintietokantoihin ja tuotantopalvelimiin. Järjestelmiin voi

piilottaa ohjelmia, jotka ottavat satunnaisesti yhteyksiä tietokantoihin ja muokkaavat satunnaisia tietueita. Lisää kaaosta voi luoda poistamalla käytöstä yrityksen keskeisiä WAN-linkkejä. Vihainen työntekijä voi ajoittaa kaiken tämän tapahtumaan samalla kellonlyömällä. (Anonymous ym. 2002, 6.)

Tuloksena saattaa olla, että organisaatio lamaantuu maailmanlaajuisesti ainakin muutamaksi päiväksi. Seuraavina kuukausina yrityksellä on vastassaan yhä uusia ajastettuja haasteita ja niitä joudutaan etsimään ja poistamaan. (Anonymous ym. 2002, 6.)

Tietoturvallisuuden ammattilaisilla on yleensä vastassaan suuri joukko raskaasti varustautuneita vastustajia. On kuitenkin olemassa työkaluja, jotka saattavat helpottaa uhkien tunnistamista. Esimerkiksi SEM-työkalun käyttö ennen uhan realisoitumista saattaa huomattavasti nostaa uhkien havaitsemisen todennäköisyyttä hyvissä ajoin. (Swift 2006, 1.)

Kun suojataan yritysympäristöjä, vastassa on paljon enemmän haasteita kuin uskotaan. Useimmat vastaantulevat ongelmat voidaan kuitenkin luokitella seuraaviin luokkiin:

- Verkon ja koneiden virheelliset asetukset
- Käyttöjärjestelmien ja sovellusten viat
- Puutteet valmistajien laadunvarmistuksessa ja vikoihin reagoinnissa
- Pätevien ammattilaisten puute (Anonymous ym. 2002, 6).

Kunnat käyttävät palveluiden tuottamisessa monien eri yhteistyötahojen rekistereiden tietoja. Näitä ovat mm. Verottaja, Kansaneläkelaitos, Väestörekisterikeskus, valtiovarainministeriö, sosiaali- ja terveysministeriö ja opetusministeriö. Näitä rekistereitä hyödyntävien palveluiden tietoturvasta huolehtiminen on kuntien vastuulla. Kuntien pitää myös asettaa toimialojensa tietojärjestelmille valtionhallinnon kanssa yhtenevät vaatimukset. Kunnat voivat käyttää apuna tätä varten luotuja VAHTI-turvallisuussopimusmalleja. (Valtiovarainministeriö 2011, 11.)

2.1 Verkon ja koneiden virheelliset asetukset

Kohteiden virheellinen konfigurointi on turva-aukkojen yleisimpiä syitä. Se voi kaataa minkä tahansa järjestelmän milloin tahansa suoritetuista turvatoimista huolimatta. Kun esimerkiksi USA:n oikeusministeriön palvelimeen murtauduttiin, oikeusministeriöllä oli käytössä palomuuri. Asiaa tutkittaessa selvisi, että väärin konfiguroitu palomuuri voi johtaa samaan lopputulokseen kuin palomuuria ei olisi käytössä ollenkaan. (Anonymous ym. 2002, 7.)

Tietojärjestelmien ja ohjelmistojen suurimpana uhkana on väärät asetukset. Virheelliset asetukset, jotka altistavat koko organisaation piileville ongelmille, voivat sijaita missä tahansa kohdassa yhteistyöverkostoa, tehtaalta aina yrityksen toimistolle asti. Esimerkiksi tietyt verkko-apuohjelmat avaavat käynnistettäessä vakavia turva-aukkoja. Monet ohjelmistotuotteet toimitetaan niin, että nämä apuohjelmat ovat oletuksena päällä. Tästä aiheutuvat riskit ovat olemassa niin kauan, että kyseinen ohjelma suljetaan tai että tehdään sen asetuksiin asianmukaisia muutoksia. (Anonymous ym. 2002, 7.)

Verkkotulostus-apuohjelmat ovat hyvä esimerkki. Ne saattavat olla asennuksen jälkeen käytettävissä, jolloin järjestelmä ei ole turvallinen. Apuohjelmien poiskytkeminen jää helposti loppukäyttäjän vastuulle. Ongelma on siinä, että käyttäjät eivät tiedä, ettei järjestelmä tai ohjelmisto ole oletusasetuksiltaan välttämättä turvallinen. Esimerkiksi sopii maailman yleisin tekstinkäsittelyohjelma Microsoft Word. Sen sisäisestä toiminnasta ei tiedetä mitään. Jos käyttäjä kirjoittaa rutiininomaisesti makroja tekstinkäsittely-ympäristössä, hän on edistynyt käyttäjä ja kuuluu pieneen käyttäjäryhmään. Useimmat ihmiset sitä vastoin käyttävät tekstinkäsittelyohjelmista vain perustoimintoja: tekstiä, taulukoita, oikeinkirjoituksen tarkistusta ja niin edelleen. Tässä käyttötavassa ei tietenkään ole mitään vikaa. Useimmissa tekstinkäsittelyohjelmissa on kuitenkin paljon kehittyneitä ominaisuuksia, joita satunnaiset käyttäjät eivät usein tunne. Tietotekniikka-alan julkaisutoiminnassa mainitaan usein tällainen sääntö: ”80 prosenttia ihmisistä käyttää vain 20% ohjelman ominaisuuksista.” (Anonymous ym. 2002, 7.)

Käyttäjät saattavat samoin tietää hyvin vähän lempikäyttöjärjestelmänsä sisäisestä toiminnasta. Useimpien käyttäjien kannalta tällaisen tietouden hankkimisessa on paljon enemmän vaivaa kuin siitä on hyötyä. Käyttäjät voivat oppia alan kirjallisuudesta tai kysymällä muilta neuvoja. Oppiminen voi olla myös työn vaatimaa, jos heidän työnsä tai muu asemansa, jossa tarjotaan runsaasti koulutusta, vaatii sitä. (Anonymous ym. 2002, 8.)

Ajan tasalla pysyminen on vaikeaa. Ohjelmistoteollisuus on dynaaminen ympäristö, ja käyttäjät ovat yleisesti ottaen kaksi vuotta kehityksestä jäljessä. Tämä viive uuden tekniikan omaksumisessa vain pahentaa tietoturvaongelmaa. Kun käyttöjärjestelmän kehitystiimi muuttaa tuotettaan oleellisesti, monien käyttäjien tietous on yhtäkkiä puutteellista. Microsoft Windows 95 on tästä hyvä esimerkki. Kun se julkaistiin, siihen oli lisätty tuki monenlaisille protokollille, joita tavanomainen Windows-käyttäjä ei tuntenut. Lisäksi rekisteripohjaiseen järjestelmään siirtyminen oli melkoinen hyppäys. On hyvinkin mahdollista, että käyttäjät eivät ole tietoisia vaikeatajuisista verkkoapuohjelmista. (Anonymous ym. 2002, 8.)

Yksi skenaario on, että käynnissä on apuohjelmia ja palveluita, joista käyttäjät eivät tiedä. Nämä palvelut voivat päälle asetettuina avata eri kokoisia turva-aukkoja. Kun tällä tavalla konfiguroitu kone on yhteydessä Internetiin, se on väärinkäyttöä odottava kohde. Tällaiset ongelmat voidaan korjata helposti. Ratkaisu on riskialttiin ohjelman tai palvelun sulkeminen tai asianmukainen konfigurointi. Eräitä tyypillisiä esimerkkejä tämänkaltaisista ongelmista ovat

- verkkotulostusohjelmat
- järjestelmän etäkonfigurointiohjelmat
- tiedostonjako-ohjelmat
- oletussalasanat
- näyte-CGI-ohjelmat ja -skriptit (Anonymous ym. 2002, 8).

Luetelluista esimerkeistä yleisimpiä ovat oletuspalvelut, kuten tiedostojen jako, tulostus ja www-pohjaiset näyteskripit, joissa on tunnettuja heikkouksia. Myös

käänteinen tilanne on mahdollinen. Sen sijaan, ettei olla tietoisia turvallisuutta uhkaavista aktiivisista palveluista, voidaan olla tietämättömiä pois käytöstä olevista ohjelmista, jotka voisivat parantaa turvallisuutta. (Anonymous ym. 2002, 8-9.)

Palveluiden tuottamisessa siirrytään entistä enemmän pilvipalvelu-ympäristöön. Tällöin saavutetaan merkittäviä hyötyjä rajapintojen ja kapasiteetin kautta. Toisaalta myös riippuvuus samoista tietoliikennepalveluista ja -tietovarastoista tulee huomioida ja varautua sen mukaan. (Valtiovarainministeriö 2011, 27.)

Monissa käyttöjärjestelmissä on sisäänrakennettuja turvaominaisuuksia. Ne voivat olla päälle kytkettyinä varsin tehokkaita, mutta aivan hyödyttömiä ennen kuin ne aktivoidaan. Tässäkin on kysymys viime kädessä asiantuntemuksesta. Jos käyttäjän tiedoissa on puutteita, hän joutuu kärsimään tarpeettomasti. (Anonymous ym. 2002, 8-9.)

Lisäksi verkon ylläpitäjä kohtaa muitakin ongelmia. Jotkut turvaohjelmat voivat olla epäkäytännöllisiä, kuten esimerkiksi turvaohjelmat, joilla voidaan hallita tiedosto-oikeuksia ja rajoittaa käyttäjien oikeuksia turvatason, kellonajan ja muiden tekijöiden perusteella. Lisää ongelmia saattaa aiheuttaa verkon pieni koko. Verkko ei välttämättä pysty toimimaan sujuvasti ja tehokkaasti, jos käytössä on kehittyneitä käyttöoikeusrajoituksia. Jos näin on, joudutaan ottamaan tämä riski ja ehkä kompensoimaan tilannetta muilla suojausmenetelmillä. Tästä tietoturvateoriassa pohjimmiltaan on kyse: pitää tehdä kompromissi riskien ja käytännön turvatoimien välillä verkkodatan arkaluontoisuuden perusteella. (Anonymous ym. 2002, 8-9.)

2.2 Käyttöjärjestelmien ja sovellusten viat

Aivan kuin kehittyneiden turvaominaisuuksien mutkikkuus ja käyttöjärjestelmien toimitus lukuisin päällekytketyin palveluin ei olisi tarpeeksi paha yhdistelmä, vielä yksi haaste on vastassa. Nimittäin virheellisestä ohjelmoinnista johtuvat turva-aukot. Näihin ei voi valitettavasti juuri vaikuttaa. Se on harmillista, koska valmistajan virheet kuuluvat yleisimpiin tietoturvaongelmien syihin. Ne, jotka

tilaavat jotain ohjelmavirhe- ja tietoturvapostituslistaa, tietävät miten yleisiä entistä vakavammat ohjelmointivirheet ovat. Yksi hyvä esimerkki tällaisesta listasta on BUGTRAQ. Verkko-ohjelmistoista löydetään päivittäin ohjelmointivirheitä eli bugeja. Niistä lähetetään joka päivä Internetiin tiedotuksia ja varoituksia. Kaikki käyttäjät eivät ikävä kyllä lue näitä tiedotuksia. (Anonymous ym. 2002, 9.)

Voidaan todeta, että järjestelmävika on mikä tahansa vika, jonka seurauksena ohjelma

- toimii väärällä tavalla, joko normaali- tai ääriolosuhteissa
- antaa murtautujan hyödyntää kyseistä puutetta tai virheellistä toimintaa ja vahingoittaa järjestelmää tai ottaa sen hallintaansa (Anonymous ym. 2002, 9).

Järjestelmävikoja on kahta päätyyppiä. Ensimmäinen tyyppi, jota kutsutaan primääriviaksi, on käyttöjärjestelmän turvarakenteessa piilevä vika. Se on tietoturvaan liittyvään ohjelmaan sisältyvä vika. Sitä hyväksikäyttämällä murtautuja pääsee yhdellä askeleella käyttämään järjestelmää tai sen dataa luvattomasti. (Anonymous ym. 2002, 9.)

On myös olemassa sekundäärivikoja. Sekundäärivika on mikä tahansa vika, joka johtuu ohjelmasta, joka ei sinänsä mitenkään liity tietoturvaan, mutta joka avaa turva-aukon järjestelmän muussa osassa. Toisin sanoen ohjelmoijille on annettu tehtäväksi kirjoittaa ohjelma, joka on toimiva, ei turvallinen. Kukaan ei ohjelman suunnittelun aikaan ole ollut huolissaan turvallisuudesta eikä ajatellut tällaisen vian mahdollisuutta. (Anonymous ym. 2002, 9.)

Toissijaiset viat ovat huomattavasti yleisempiä kuin ensisijaiset viat, erityisesti alustoilla, joissa tietoturva ei ole ollut keskeinen tekijä. Esimerkki sekundäärituryaviasta on jokin vika sellaisessa ohjelmassa, joka tarvitsee erityisoikeuksia tehtäviensä suorittamisessa eli ohjelmassa, joka pitää ajaa root- tai pääkäyttäjän oikeuksilla. Jos hyökkäys voidaan kohdistaa tällaiseen ohjelmaan, murtautuja voi tämän ohjelman kautta saada erityisoikeuksia tiedostoihin ja palveluihin. (Anonymous ym. 2002, 9.)

Sekä primääriset että sekundääriset järjestelmäviat ovat Internet-yhteisölle erityisen vaarallisia, kun niitä esiintyy päivittäin käytettävissä sovelluksissa ja protokollissa kuten FTP:ssä, DNS:ssä, SSH:ssa tai Telnetissä. Nämä tehtäväkriittiset sovellukset muodostavat Internetin sydämen, eikä niitä voida yhtäkkiä poistaa, vaikka niissä ilmenisi turvallisuusvikoja. (Anonymous ym. 2002, 9.)

Tämä käsite on helpommin ymmärrettävissä, kun kuvitellaan mitä tapahtuisi, jos Microsoft Word havaittaisiin täysin turvattomaksi. Wordin käyttöä ei lopetettaisi vain sen vuoksi, sillä miljoonat organisaatiot ympäri maailmaa ovat riippuvaisia Wordista. Mutta siinä, onko vakava turvallisuusvika Microsoft Wordissa vai vakava turvallisuusvika Apache-www-palvelimessa, on valtava ero. Vakava vika Apachessa saattaisi satoja tuhansia palvelimia ja näin ollen miljoonia käyttäjätunnuksia riskialttiiksi. Internetin koon ja sen nykyään tarjoamien palvelujen vuoksi Internetin turvarakenteeseen sisältyvät viat ovat kansainvälisen tason huolenaihe. (Anonymous ym. 2002, 9-10.)

Organisaation toiminnan jatkuvuuden takia tulee varautua ICT-toiminnan häiriötilanteisiin. Häiriötilanteet voivat johtua esim. luonnonilmiöstä, tietojärjestelmävirheestä, onnettomuudesta, laiteviasta, sähkökatkosta, tietokatkosta ja toiminta- tai käyttövirheestä. Häiriö voi olla myös tahallaan aiheutettu. Tietoverkkoon saatetaan hyökätä, tehdä vahinkoa sen laitteille ja järjestelmille sekä yleistä ilkivaltaa estämällä verkon toiminta. (Valtiovarainministeriö 2011, 33.)

2.3 Puutteet valmistajien laadunvarmistuksessa ja vikoihin reagoinnissa

Esimerkkinä mainittakoon keskustelu Microsoftin edustajien ja erään heidän suuren asiakkaansa välisessä kokouksessa. Kokouksen aikana tuli puheeksi Exceliin piilotettu lentosimulaattori. Asiakas halusi tietää, miksi taulukkolaskentaohjelmassa oli lentosimulaattori. Hän halusi tietää, kuinka paljon tilaa se vei ohjelmassa, muistissa ja yrityksen työasemissa. Mutta ennen kaikkea hän halusi tietää, miten se oli päässyt Microsoftin laadunvarmistuksen ja -valvonnan ohi. Muutama koodirivi olisi ehkä ymmärrettävää, mutta kokonainen lentosimulaattori on aivan eri asia. Microsoft vastasi, että he tiesivät koko ajan sen olemassa-

olosta ja että tämä ”pääsiäismuna” oli vain asia, jonka he antoivat Redmondin ohjelmoijien tehdä huvin vuoksi. ”Se kuuluu ohjelmistonkehityskulttuuriin”, sanoivat Microsoftin edustajat. (Anonymous ym. 2002, 11.)

Niin kauan kuin ohjelma toimii odotetulla tavalla ja tuottaa oikeaa tietoa, sen sisältämään ohjelmointiin ei kiinnitetä huomiota. Useat ohjelmistot ovat vielä suljetun lähdekoodin alaisia, jolloin ohjelman lähdekoodia ei pysty ulkopuolinen tarkastamaan.

Monilla ohjelmistoyrityksillä ei ole riittäviä laadunvalvonta- ja laadunvarmistuskäytäntöjä. Microsoft on helppo kohde, koska se on tuonut markkinoille niin monia ohjelmistotuotteita, mutta totuus on, että monet yritykset ovat tehneet samanlaisia virheitä. Organisaatiot ja loppukäyttäjät kärsivät, kun verkkoihin murtaudutaan näitä erehdyksiä hyväksikäyttäen. Valmistajat kuitenkin väittävät, että heidän asiakkaansa haluavat lisää ominaisuuksia eivätkä parempaa turvallisuutta. (Anonymous ym. 2002, 12-13.)

Teknisesti tai fyysisesti huonosti suojatut palvelut (ml. tieto, sovellukset, tietoverkot ja järjestelmät) voivat olla tietojen urkinnan kohteena. Tietojärjestelmät saattavat olla myös haltuunottoyritysten tai palveluiden lamauttamisen kohteina. (Valtiovarainministeriö 2011, 33.)

Näihin asioihin pyritään nykyisin vaikuttamaan yhä enemmän koulutuksella ja erilaisilla ohjeilla. Yhtenä uusimmista ohjeistuksista on National Institute of Standards and Technologyn Special Publication 800-160 Systems Security Engineering (Ross ym. 2014).

2.4 Pätevien ammattilaisten puute

Jos valmistaja ja ohjelmoijat eivät tuottaisi virheitä sisältävää koodia, käyttöjärjestelmiä ei toimitettaisi kaikki mahdolliset palvelut oletuksena sallittuina ja käynnissä. Jos kaikkialle ei olisi asennettu näyteskriptejä eivätkä ihmiset tekisi jatkuvasti vääriä asetuksia ja erehdyksiä, meillä olisi silti yksi suuri ongelma - tarpeeksi monilla ihmisillä ei ole kokemusta tietoturvasta. Organisaatioiden joh-

dolla on nykyään vaikeuksia pätevien verkkoinsinöörien, järjestelmien ylläpitäjien ja ohjelmoijien löytämisessä, tietoturva-ammattilaisista puhumattakaan. (Anonymous ym. 2002, 16.)

Osaaminen koostuu mm. organisoinnista, henkilöiden ammattitaidosta, perehtyneisyydestä, ohjeistoista, dokumentaatiosta, ongelmaratkaisutaidoista, käytettävyydestä sekä tukijärjestelmien tietokannoista, esim. ServiceDesk. (Valtiovarainministeriö 2011, 23.)

Asiaa pahentaa vielä se, ettei voida hankkia koulutusta, joka tekee tavallisesta käyttäjästä välittömästi tietoturva-ammattilaisen. Osaaminen pitää hankkia vaiheittain. Ensin pitää saada hyvät tiedot reitittimistä, kytkimistä ja palomuureista ja opetella eri käyttöjärjestelmät läpikotaisin. Lisäksi pitää oppia tiedon salaamisen ja ohjelmoinnin perusteet ja hankkia vankka ymmärrys TCP/IP:stä. Sen jälkeen voidaan aloittaa tietoturvaan liittyvien hienouksien, tapausten selvittämisen ja muiden toimien opiskelu. (Anonymous ym. 2002, 16.)

Resurssit jatkuvuuden hallinnalle ja tiedon turvaamiselle on koettu rajallisiksi. Joissain kunnissa tämä näkyy taloudellisena rajoitteena, ja toisissa taas suurin rajoittava tekijä on henkilöresurssien saatavuus. Suurimmalta osalta kuntia ICT-jatkuvuuden ja erityistilanteiden suunniteltu hallinta puuttuu tai dokumentointi on ollut päivittämättä vuosia. (Valtiovarainministeriö 2011, 41.)

Osaavan henkilöstön puutteen johdosta joidenkin organisaatioiden tietoturvaohjelmat ovat väärin suunniteltuja tai niitä ei ole lainkaan. Käytännöt ovat epätäydellisiä tai puuttuvat kokonaan. Yrityksissä ei ole tehty uhkien arviointia. Koneisiin ei asenneta korjauspaketteja, kehityshankkeet epäonnistuvat, lokeja ei seurata eikä käyttäjiä kouluteta. (Anonymous ym. 2002, 16.)

Tilanteen ei kuitenkaan tarvitse olla tällainen. Jos ylläpitäjät ja käyttäjät huolehtisivat vastuualueistaan tietoturvan suhteen, ei tarvittaisi kaikkitietävien tietoturvagurujen armeijaa. Odotetaan päivää, jolloin turvakäytännöt ovat yhtä tavallinen asia kuin järjestelmän varmuuskopiointi ja kuuluvat jokaisen hyvän ylläpitäjän työnkuvaan. (Anonymous ym. 2002, 16.)

Kunnille tuottaa erityisesti haasteita palvelujen jatkuvuuden hallinta. Useat osapuolet muodostavat palvelutuotantoverkoston. Vaatimusmäärittelyt, rajapinnat, toimintatavat, epäyhtenäinen henkilöstö ja osaaminen asettavat valtavat haasteet koko organisaatiolle. Jo palveluiden suunnittelu- ja hankintavaiheessa tulee määritellä tarkasti kaikkien osapuolten riskienhallintaan liittyvät vastuut häiriötilanteissa. (Valtiovarainministeriö 2011, 22.)

Lyhyesti sanottuna ongelmana on se, että yritykset pyrkivät olemaan retroaktiivisia tietoturvan suhteen. Odotetaan suurta onnettomuutta ja kun se sattuu, selvitetään, miten minimoidaan tappiot. Julkaistaan lehdistötiedote, jossa kerrotaan tapahtumasta hyvin niukasti ja toivotaan, että media unohtaa koko tapauksen. Se, että käyttäjien kaikki tiedot on murrettu tietokannasta ja salasanat on salattu ilman tietoturvallista suolausta ja sattumanvaraista merkkijonoa, tarkoittaa sitä, että salasanojen murtaminen on vain ajan kysymys. Parhaassa tapauksessa yritys panostaa aktiivisesti tietoturvaan, jolloin ongelmat eivät ikinä riistäydy käsistä ja jatkuvalla tietoturvan hallinnan parantamisella saavutetaan kustannustehokkain vaihtoehto.

2.5 Tietoturvakoulutuksen tärkeys

Tietoturvaihmiset ovat perinteisesti yrittäneet pitää tietoturvallisuuteen kuuluvan tietotaidon poissa tavallisen käyttäjän ulottuvilta. Tietoturva-asiantuntijat ovat IT-maailmassa arvostetussa asemassa. Heitä pidetään vaikeatajuisen tiedon osaajina, jota tavallisen käyttäjän ei ole tarpeen osata. Yhteen aikaan tästä lähestymistavasta oli etua: käyttäjillehän pitäisi antaa tällaista tietoa vain silloin, kun siihen on tarvetta. Nyt tavallinen käyttäjä on kuitenkin sellaisessa tilanteessa, että hän tarvitsee tietoa. (Anonymous ym. 2002, 16.)

Pitääkö käyttäjän ottaa verkkoturvallisuus vakavasti, riippuu hänen asemastaan. Jos olet kauppias, kysymykseen on helppo vastata: jotta voit käydä verkossa kauppaa, sinun pitää huolehtia hyvästä tietoturvasta. Kukaan ei osta palveluja Internetistä, ellei hän voi tehdä sitä turvallisin mielin. Tämä johtaa asiakkaan ongelmaan: miten internetin verkkokauppa saadaan luotettavaksi, kun murtau-

tujat pystyvät kaappaamaan arkaluontoisia tietoja. Kuluttajan ja kauppiaan välissähän on vielä yksi tietoturvasta huolehtiva osapuoli: ohjelmistovalmistaja, joka tarjoaa kaupankäynnin mahdollistavia työkaluja. Nämä osapuolet ja heidän syynsä turvallisuudesta huolehtimiseen ovat ilmeisiä. Sen lisäksi on kuitenkin olemassa vähemmän näkyviä näkökohtia. (Anonymous ym. 2002, 16.)

Yksityisyys on eräs huolenaihe. Internet on ensimmäinen konkreettinen todiste siitä, että orwellilainen yhteiskunta voisi toteutua. Jokaisen käyttäjän pitäisi ymmärtää, että salaamaton tietoliikenne Internetissä on täysin turvatonta. Vaikka Internet on hyvä resurssi tutkimusta tai huvia varten, ei se ole luotettava ystävä. (Anonymous ym. 2002, 16.)

ENISA on Euroopan Unionin oma vastaus tietoturvaongelmiin. Organisaation päämääränä on olla tietoturvallisuuden alalla tiedon jaon, parhaiden käytäntöjen ja tietämyksen keskus. (ENISA 2014.)

Organisaation oma osaaminen yhdessä palveluja tuottavan toimittajaverkoston kanssa muodostavat perustan varautumiselle. Palvelujen tuottajat ja infrastruktuurin ylläpitäjät tekevät usein vain välttämättömimmän: Noudatetaan palvelutasosopimuksissa olevia vaatimuksia ja muuten toimitaan oman tarpeen mukaisesti. Usein tukijärjestelmän ja erikoiskomponenttien vaatima erityisosaaminen on saatavissa vain valmistajan kautta. (Valtiovarainministeriö 2011, 59.)

3 TIETOTURVALLISUUDEN MITTAAMINEN

Tietoturvallisuuden hallintajärjestelmää pitää mitata, seuraavien syiden vuoksi:

- Voidaan parantaa tietoturvallisuuden tasoa organisaatiossa.
- Pystytään osoittamaan johdolle, mitä lisäarvoa tietoturva tuo organisaatiolle.
- Voidaan lisätä tietoturvallisuuden toiminnan näkyvyyttä.
- Kyetään todentamaan säännösten ja lakien tuomien vaatimuksien toteuttamisen taso. (Hayden 2010, 4).

Tietoturvan mittaamisesta käydään paljon keskustelua. Jotkut saattavat olettaa tietoturva-asioiden mittaamisen olevan keksityn vasta vuonna 2010. Asia ei suinkaan ole näin, sillä tunnettuja tietoturvamittareita kuten ALE (annual loss expectancy), TCO (total cost of ownership) sekä kvantitatiivinen ja kvalitatiivinen riskikartoitus, on ollut vuosia alan ammattilaisten käytössä. Uutena asiana tietoturvallisuuden mittaamisessa on se, että perinteiset tavat mitata eivät ole enää riittäviä. Niistä ei saa tarvittavaa tietoa tukemaan päätöksentekoa tai osoittamaan tietoturvatoimien tarpeellisuutta. Ne eivät ole riittäviä muuttuvassa tietoturvakentässä, jossa uhat ovat hienostuneempia ja vastuut sekä vastuiden noudattamisen tarkastukset lisääntyvät. Samaa mieltä ollaan siitä, että mittaamista on parannettava ja on ideoitava uusia tapoja analysoida jo olemassa olevaa tietoturvallisuuden mittaamisen mittausdataa. (Hayden 2010, 4.)

Ongelmana on, että mitattaessa keskitytään asioihin, joiden kanssa olemme päivittäin tekemisissä, ja lopulta päätetään, että vain niillä mittauksilla on merkitystä. Jos esimerkiksi analysoidaan palomuurien lokitiedostoja, eikä ymmärretä miten muut tietoturvallisuuden mittaamisen avainhenkilöt mittaavat tietoturvallisuutta tai muita liiketoiminnalle tärkeitä arvoja, ei pystytä käyttämään analyysin dataa päätöksenteon tukena. Kun yrityksessä on opittu, miten tietoturvallisuuden eri avainhenkilöt määrittelevät onnistuneen mittauksen, voidaan tietoturvan mittaamisesta saatua dataa käyttää parantamaan heidän toimintaansa ja samalla demonstroidaan tietoturvan mittaamisen arvoa. (Hayden 2010, 4-5.)

Tietoturvan muuttuessa monimutkaisemmaksi ja laaja-alaisemmaksi tietoturvallisuuden asiantuntijoiden vastuualue kasvaa yrityksen pelkän pääoman suojaamisesta taloudelliseen menestykseen ja kilpailukyvyn kasvattamiseen. Tieto siitä, miten tietoturva toimii, tulee olemaan maailmanlaajuisesti ja strategisesti tärkeää. (Hayden 2010, 4-5.)

3.1 Mittarit ja mittaaminen

Perimmäinen syy mittaamiselle on sama kuin kaikessa, mitä mitataan: halutaan ymmärtää asioita paremmin. Tietoturvallisuutta mitataan, koska halutaan ymmärtää tietoturvaan liittyviä asioita. Tämä saattaa vaikuttaa yksinkertaiselta, mutta käytäntö osoittautuu vaikeammaksi, miltä alkuun näyttää. Esimerkiksi organisaatiolla on käytössä tietoturvallisuuden mittaamissuunnitelma, mutta se silti kamppailee ymmärtääkseen miten organisaation tietoturvapyrkimykset vaikuttavat tietoturvallisuuden tasoon. Usein tämä johtuu siitä, että mittaamissuunnitelma on itse asiassa datankeruusuunnitelma, eikä mittaamislähtöinen alkuunkaan. Tietoturvadatan kerääminen on tärkeää mille tahansa tuloksia tuottavalle mittaamissuunnitelmalle. Mutta ilman asiayhteyttä dataan ja ideaan siitä, miksi sitä kerätään ja mitä sillä aiotaan tehdä, saatetaan päätyä kuvailemaan mittaamisponnisteluja pelkästään teratavuina lokitiedostoja ja hyllyinä täynnä auditointiraportteja. (Hayden 2010, 5.)

Yksi yleisimpiä virheitä, joita tehdään tietoturvallisuuden mittaamissuunnitelman toteuttamisessa on, että keskitytään liikaa mittareihin itsessään. On tärkeää korostaa, että tietoturvamittaristo on matka eikä päämäärä. Kun on luotu tietoturvallisuuden mittaamissuunnitelma, tulee kysyä, miten mittaamisen tulokset parantavat tietoturvajärjestelmien ja prosessien ymmärtämistä. Ymmärtäminen ei ole vianmääritystä. Tieto siitä, että vuodesta toiseen jokin prosentti käyttäjien salasanoista on helposti murrettavissa tai että haavoittuvaisten internetpalvelimien suhde ei ole laskenut alle 25%, vähentää kyllä epätietoisuutta tietoturvallisuuden toimivuudesta, mutta jotain puuttuu tietoturvallisuuden hallintaohjelmasta. Vaikka tietoturvan taso kohenisi, mutta ei voida osoittaa kohenemisen syytä,

ovat mittarit arvottomia. Mittarit ovat datavarastoja, ne määrittelevät ja standardisoivat informaatiota. Mittarit eivät organisoi informaatiota tietämykseksi sen enempää kuin hyvin määritellyt sanalistat muuttavat sanakirjan kirjallisuudeksi. Tämä voidaan saavuttaa vain ihmisten avulla. (Hayden 2010, 5.)

Olen sitä mieltä, että yrityksen mittariston tulisi olla PDCA-mallin mukainen ja johtaa jatkuvaan mittariston ja mittaamisen kehittämiseen. Tähän päästään luomalla kaksi mittaristoa. Johdon mittaristo ja tietoturvasta vastaavan, usein tietoturvapäällikkö, mittaristo. Johdon mittaristo keskittyy yrityksen kannalta olennaisiin riskeihin kustannuksia ja julkisuuskuvaa painottaen. Tietoturvapäällikön mittaristo esittää kokonaiskuvan, miten tietoturvallisuuden hallintajärjestelmä toimii ja miten sitä tulisi kehittää. Molemmat mittarit ovat sidoksissa toisiinsa siten, että yhdellä mittarilla mittaaminen vaatii myös toisella mittarilla mittausta.

3.2 Mittaaminen on toimintaa

Tietoturvallisuuden mittareiden päämääränä ei ole kerätä valtavasti dataa. Pieni datajoukko, jota ymmärretään hyvin ja hyödynnetään säännöllisesti, on paljon arvokkaampi kuin vuori käsittelemätöntä dataa. Mittareiden todellinen hyöty saavutetaan silloin, kun niiden antama data auttaa toimimaan päämäärän saavuttamiseksi. Mittareiden tulisi olla havaintojen dokumentaatio. Mittaaminen on tehtäväkokonaisuus, johon kuuluu havaintojen tekeminen ja datan kerääminen käytännönläheisen tiedon saavuttamiseksi siitä, mitä yritetään ymmärtää. Tämä erovaisuus on tärkeää, sillä mittarit eivät anna vain informaatiota tietoturvasta vaan aiheuttavat myös kuluja ja riskejä. Mittariston tuottaman datan kerääminen vain datan keräämistä varten ei ole mittaamista, paitsi jos keräämisen alkuperäisenä tarkoituksena on aiemman datan tutkiminen mahdollisten lainalaisuuksien löytämiseksi. (Hayden 2010, 6.)

Tietoturvallisuuden mittaamisen riskinä ovat samat asiat kuin minkä tahansa asian kanssa, jota ymmärretään nyt paremmin kuin ennen. Tieto voi olla valtaa, mutta pysyäkseen tietona, siihen liittyy vaatimuksia ja velvoitteita. Työn lisäksi, mikä aiheutuu mittausdatan keräämisestä ja varastoinnista, on huomioitava mit-

tausdatan keräämisen seuraukset. Haavoittuvuusdatan kerääminen järjestelmistä aiheuttaa sen, että tiedetään miten heikkoja ne mahdollisesti ovat. Koska nämä tiedot kirjataan ylös joko manuaalisesti tai automatisoidun ohjelman toimesta, raportti sijaitsee joko hyllyssä tai kiintolevyllä. Tietoturvamurron sattuessa nämä mittausraportit saatetaan löytää mahdollisen oikeustapauksen tutkinnan yhteydessä. Ongelman tietäminen ja sen asian huomioimatta jättäminen, jonka johdosta tietoturvamurto tapahtui, saattaa olla vahingollisempaa kuin tietämättömyys ennen mittaamista. Monet organisaatiot eivät ota huomioon mahdollisuutta, että kerätty data luo organisaatiotason tallenteen mahdollisesti myöhemmin löydettäväksi. Käyttämätön mittausdata pahentaa asiaa entisestään. Ei ainoastaan jouduta tietomurron kohteeksi vaan joudutaan myös vastaamaan sen seurauksista, sillä organisaation katsotaan tunteneen tämän uhan. (Hayden 2010, 6-7.)

Asian ydin ei ole se, että mittaaminen on liian riskialtista tai tuomitsevaa, vaan se, että jos dataa kerätään eikä sitä käytetä, silloin ei ole kyse tietoturvallisuuden hallintajärjestelmän mittaamissuunnitelmasta. Mittaaminen ilman analyysiä ja siihen perustuvia toimia tuhlaa aikaa ja rahaa ja lisää epävarmuutta sekä riskejä niiden vähentämisen sijaan. (Hayden 2010, 7.)

Organisaation koko yhteistyöketjun tulee tietää enemmän organisaation tietoturvakäytännöistä. Yhtenäiset minimivaatimukset koko yhteistyöverkostossa varmistavat tietoturvallisen perusmallin, jolloin ongelmia syntyy vähemmän tai ne ovat lievempiä. Tietoturvallisuuden sanotaan olevan niin vahva kuin sen heikoin lenkki. Mikään ei ole haastavampaa kuin yrittää parantaa yhteistyökumppaneiden tietoturvataitoa ja -tietoisuutta ilman, että häiritsee sujuvaa jokapäiväistä toimintaa.

Organisaation tulisi huomioida tietoturvavaatimukset, myös alihankkijoidensa koko ketjussa. Läpinäkyvyyden lisääminen koko hankintaketjuun lisää myös kustannuksia kaikille osapuolille. Lisääntyneet kustannukset saattavat olla suurin este tietoturvallisuuden etenemiselle. (NIST 2013, 45.)

Tietoturvaprosessien ymmärtämisestä saatava hyöty on paljon suurempi kuin ymmärtämiseen liittyvät riskit. Mittareiden pitää perustua järkevälle tietoturvallisuuden mittaamisstrategialle sekä käytännön soveltamiselle, ei datan keräämiseksi sen itsensä vuoksi. Ilman datan analyysiä ei tule muuttaa organisaation toimintaa. Tietoturvallisuuden mittaaminen tulisi nähdä osana liiketoimintaprosessia, joka pyrkii jatkuvasti parantamaan yrityksen informaatiopääoman suojaamista. (Hayden 2010, 7.)

Tietoturvallisuuden mittaamissuunnitelman suunnittelussa tulee käyttää samaa kriittistä silmää riskeihin, kustannuksiin ja hyötyihin kuin mihin tahansa muuhun liiketoimintaprosessiin. Yrityksen seuraamaa jokaista mittaria kohden jonkun tulee ymmärtää, miksi juuri sitä dataa kerätään ja mihin päätöksiin dataa käytetään tukena. On sallittua ja usein hyödyllistäkin kerätä tutkimusdataa, jolle ei ole suoraan hyödynnettävää päämäärää, mutta tutkimusmittareidenkin tulee olla ymmärrettävissä ja niiden tulisi lopulta johtaa uuteen tietoon ja ymmärrykseen. (Hayden 2010, 7.)

Otettaessa mittaristoa käytäntöön tietoturvatoimintojen ymmärtämiseksi tulee vastata kysymykseen, ollaanko organisaatiossa valmiita toiminaan mittausohjelman tuottaman tiedon mukaan. Tulokset voivat olla odottamattomia tai ne voivat aiheuttaa uusia velvoitteita ja vaatimuksia tietoturvallisuuden toiminnalle. Jos ei olla valmiita toimimaan selville saadun tiedon mukaan, mittarit ainoastaan tekevät ongelmista monimutkaisempia. (Hayden 2010, 7.)

3.3 Tietoturvamittarit tänä päivänä

Huolimatta lisääntyneestä mielenkiinnosta IT tietoturvamittareita kohtaan, tietoturva-ala käyttää jo useita yleisesti tunnistettuja mittareita. Jotkin näistä mittareista ovat tietoturvakäytäntöjen kulmakiviä niin tuotemarkkinoinnissa kuin riskienhallinnassa ja tietoturvan kehittämisessäkin. Ongelmana monissa näissä mittareissa ovat niiden rajoitteet, jotka aiheuttavat harhaanjohtavia osoittimia tietoturvallisuuden toimivuudesta. Haydenin (2010, 8) mukaan mikä tahansa empiirinen mittaus, joka auttaa vähentämään epätietoisuutta organisaatiossa on

hyvä mittari. Hän ei usko, että mittari tulisi jättää huomiotta vain siksi, ettei se ole kvantitatiivinen tai spesifinen. Mittari saattaa olla hyvä yksinkertaisesti siksi, että se on helppo ja yksiselitteinen. Mikä tahansa mittaus aiheuttaa ongelmia, kun se suoritetaan huonosti ja kun mittaajat eivät ole tarpeeksi kriittisiä metodejaan kohtaan. Ongelmat, jotka voivat aiheutua huolimattomista tietoturvallisuuden mittaamisyrityksistä, saattavat johtua ongelmista datan laadussa ja empiirisessä täsmällisyydessä, tai siitä, että mittareita käytetään väärällä tavalla.

3.4 Riski käsitteenä

Riski on peruskäsitteitä tietoturvallisuudessa. Jokaisen tietoturvaan liittyvän kysymyksen ytimessä on perustavampi kysymys siitä, mitä riskejä otamme tehdessämme tietyn valinnan tai kun valitsemme tietyn toimintatavan. Riski on ensimmäisenä listalla kysyttäessä tietoturvallisuudesta vastaavilta henkiöiltä: kerro huolesi. Niin kriittistä kuin riskin ymmärtäminen onkin, se on usein yksi huonoiten ymmärretty käsite. Tietoturvallisuuden ammattilaiset usein käyttävät termejä kuten *riskikartoitus*, *riskianalyysi* ja *riskienhallinta* yleiskäsitteinä, joissa riskin määritelmä yleensä oletetaan tunnetuksi tai sitä pidetään itsestäänselvyytenä.

Tietoturvallisuudessa riski tyypillisesti yhdistetään johonkin vahinkoon tai järjestelmien tai datan tuhoutumiseen, mutta tämä määritelmä on liian ylimalkainen, eikä se ole yleisesti hyväksytty tai jatkuvassa käytössä. Sen sijaan, riski yleensä yhdistetään muihin yhtä yleistäviin uhkakuviin, haavoittuvaisuuksiin ja parametreihin, jotka ovat usein yhtä epätarkkoja kunnes jäljelle jää epäselvä konsepti, joka voi muuttua läpi organisaatioiden ja toteutusten. Tästä syystä on vaikea johdonmukaisesti mitata riskiä. Asiaa ei helpota se, että monet tietoturvatoimittajat hämmentävät termiä tai väärinkäyttävät sitä myydäkseen tietoturvatuotteita ja -palveluita. Termiä *riski* käytetään kuvamaan monia eri ilmiöitä, joiden tiedetään vaikuttavan turvallisuuteen, mutta joita ei ole vielä tutkittu ja määritetty. (Hayden 2010, 8.)

Mielestäni julkishallinto näkee riskin toisessa valossa. Riskin todennäköisyys ja vakavuus ei ole pelkästään dokumentoitava asia. ICT-varautumisen ydin on selvitä mahdollisimman hyvin katastrofista. Tämä on todella hyvä periaate.

Varautumiseen kuuluu ICT-riskeihin valmistautuminen ja niistä aiheutuvien häiriötilainteiden hallinta. Riskianalyysissä otetaan huomioon organisaation suojattavat kohteet, uhka-arvio, haavoittuvuus- ja vaikuttavuusnäkökulma. Riskianalyysin pohjalta tehdään ICT-varautumisen vaatimukset, päätetään ennakoivat suojaustoimenpiteet, sovitaan miten hallitaan häiriötilanteet ja miten toiminta palaa normaaliksi. Vahinkojen minimoimiseksi tehdään jatkuvuussuunnitelma johdon toimesta. Tällöin saadaan perusta valmiussuunnitelmalle poikkeusoloja varten. (Valtiovarainministeriö 2011, 21-22.)

Jatkuvuuden hallinta nähdäkseni tarvitsee avukseen tietoturvallisuuden mittausta. Resurssien käyttö on tehokkaampaa, kun ongelmiin puututaan mahdollisimman aikaisessa vaiheessa. Lisäksi ratkaisemalla nopeasti ja päättäväisesti tietoturvaongelmia, innostetaan koko organisaation henkilökuntaa raportoimaan rohkeasti tietoturvapoikkeamista.

Teoreettisen riskin määrittely riskiarvioinnin ja riskianalyysien kautta saattaa onnistua, mutta jos ei ymmärretä, miten tietoturvallisuuden hallintajärjestelmät ja prosessit oikeastaan toimivat ja miten ne pannaan käytäntöön, organisaatio ei voi tuntea todellista altistumistaan riskeille. (Pagett & Ng 2010, 1.)

Mainittaessa riski tietoturvallisuuden kontekstissa jokainen on samaa mieltä sen tärkeydestä, mutta varmoja ei voida olla siitä, että jokainen ajattelee riskistä samalla tavalla. Riski voi kuitenkin tarkoittaa monia eri asioita. Kysyttäessä rahoitusalan ammattilaiselta riskistä, saatetaan aluksi kysyä, mitä tarkoitat. Puhutaanko riskeistä, joihin voi itse vaikuttaa, vai riskeistä joihin ei voi vaikuttaa? Puhutaanko riskeistä, jotka muuttuvat jonkin todennäköisyyskäyrän mukaan, vai onko riskin todennäköisyys määrittelemätön. Mittaaminen paranee harjoittelulla ja kurinalaisuudella, ja mitä enemmän tietoturvallisuuden ammattilaiset yrittävät mitata ja ymmärtää organisaation päivittäistä toimintaa, sitä paremmaksi arvi-

ointi muuttuu. Luultavasti yleisin tapa mitata tietoturvariskejä on käyttää jotain variaatiota ”Todennäköisyys x Vakavuus”-taulukosta. (Hayden 2010, 9.)

Taulukko 1. Yleistetty riskikartoitustaulukko (Hayden 2010, 10).

		Tapahtuman todennäköisyys		
		Korkea	Keskitaso	Matala
Tapahtuman vakavuus	Korkea	”Olemme tuhon omia”	Huono	Ääritapaus
	Keski-taso	Huono	Ei hyvä	Virhe
	Matala	Harmi	Tyypillinen	”Ei merkitystä”

Yllä oleva taulukko voi olla monimutkaisempi ja sisältää erilaisia asteikoita, painokertoimia, värikarttoja, tai muita asioita, mutta kaikki ovat mukaelmia samasta konseptista. Ideana on arvioida todennäköisyys sille, että jokin tieto-omaisuus joutuu negatiivisen tietoturvatapahtuman kohteeksi, ja sen jälkeen arvioidaan, miten vakavasti tapahtuma vaikuttaa siihen. Matriisi täytetään tulosten mukaan

ja siten saadaan priorisoitu riskiyhteenveto. Taulukko on yksinkertainen ja helposti ymmärrettävä, minkä vuoksi se on säilyttänyt vahvan asemansa pitkään. Siitä huolimatta, tietoturvallisuuden riskien mittaamisessa se on kohtalaisen rajoittunut. Erityisesti se on liian rajoittunut käytettäväksi joidenkin tietoturvaan liittyvien päätösten tukena. (Hayden 2010, 10.)

Varsinaisen riskin mittaamisen puutteista huolimatta matriisi voi olla tehokas väline kohdennettuna kyselytutkimuksena. Sen avulla tietoturva-asiantuntijat voivat nopeasti luoda prototyyppejä siitä, minkä he uskovat olevan suurimpia tietoturvaongelmia. Asian ydin on, että asiantuntijoilla pitäisi olla asiantuntevampia mielipiteitä omalta osaamisalueeltaan kuin muilla. Tulee huomata, että mielipiteellä voi olla yksistään arvoa, eikä vaatia sitä, että mielipiteen pitää perustua faktoihin ollakseen arvokas. Riskikartoitustaulukko asiantuntijoiden tekemänä voi olla hyödyllinen arvio, mutta se on silti vain muutama mielipide riskistä. Suurimmat riskimatriisissa tunnistetut tietoturvaongelmat eivät välttämättä ole suurimpia organisaatiota uhkaavia tietoturvaongelmia. (Hayden 2010, 10). Mielestäni jokainen ihminen näkee riskit oman suodattimensa lävitse ja se vääristää koko riskienkartoitusmetodia.

3.5 Riskikartoituksen ongelmat

Tietoturvallisuuden riskikartoituksen metodologiaan liittyy monia asioita. Esimerkiksi organisaation vastuuhenkilöistä kootut ryhmät joko kootaan yhteen tai kysytään kyselylomakkeilla riskiarviot tapahtumien todennäköisyyksille sekä niiden vakavuudelle riippuen järjestelmistä ja datasta. Nämä yksilöt velvollisuudentuntoisesti tuottavat pyydetyn datan, jolla täytetään matriisi. Lopputuloksena on keinotekoinen todiste siitä, että mittaaminen on suoritettu. Kartoituksen tekijät voivat jopa yrittää väittää, että mittaaminen oli empiiristä, koska se sisälsi jonkin ilmiön havainnointia. (Hayden 2010, 10.)

Riskinarvioiminen ei ole sen mittaamista. Riskin painoarvo riippuu jokaisen osallistujan omasta perspektiivistä. Ongelmia syntyy, kun jokainen on sitä mieltä, että oma arvio riskistä on oikein, tärkein ja vaatii suurimman varautumis- ja toi-

mintastrategian. Tämän takia jo valmiiksi niukka tietoturvabudjetti on riittämätön todennäköisempien uhkien torjuntaan. Organisaatiossa tulee keskittyä siihen, mikä aiheuttaa eniten laajemmassa mittakaavassa ongelmia. Ei siihen, mikä yksittäinen ongelma voi maksaa eniten. Mittaamalla riskienarvioimisen ja riskien toteutumisen korreloimista saavutetaan tarkempi kuva todennäköisimmistä organisaatiota kohtaavista ongelmakohdista.

4 TIETOTURVAN MITTAAMISEN STANDARDI

Tietoturvan mittaamisen standardi sisältää suosituksia ja ohjeistusta siihen, miten tietoturvallisuuden mittaaminen tulisi toteuttaa, miten mitata ja miten käyttöön otetut ISO/IEC 27001-standardin mukaiset kontrollit ovat tehonneet (ISO/IEC 27004:2009, vi).

Standardi ISO/IEC 27001:2013 velvoittaa organisaatiota säännöllisesti arvioimaan tietoturvallisuuden hallintajärjestelmän toimivuutta siitä saatuihin mittaustuloksiin pohjautuen. Mittaamalla voidaan todentaa, että tietoturvavaatimukset on saavutettu, sekä varmistaa vertailukelpoiset ja toistettavat mittaustulokset. Se, miten organisaatio saavuttaa ISO/IEC 27001:ssä määritetyt mittausvaatimuksensa, riippuu monesta muuttujasta, kuten organisaatioon kohdistuvista tietoturvariskeistä, organisaation koosta, käytettävissä olevien resurssien määrästä sekä soveltuvista juridisista, sopimuksellisista ja muista asetuksiin perustuvista vaatimuksista. Metodit, joilla mittausvaatimukset täytetään, tulee valita huolellisesti ja oikeutetusti. Näin vältetään ylimääräisten resurssien käyttö, joka on muilta tietoturvanhallintajärjestelmän osilta pois. Parhaassa tapauksessa mittaustoiminnan tulisi olla osa jokapäiväistä toimintaa, vieläpä minimaalisella lisäresurssien tarpeella. (ISO/IEC 27004:2009, vi.)

Tässä kansainvälisessä standardissa annetaan suosituksia, miten organisaatio voi täyttää ISO/IEC 27001:ssä määritetyt vaatimukset ja luoda seuraavien toimien mukaan perustan tietoturvan mittaamiselle:

1. Suureiden luominen (mm. perussuureet, johdetut suureet ja indikaattorit)
2. Tietoturvallisuuden mittausohjelman käyttöönottaminen
3. Tietoturvallisuuden mittausohjelman toimiminen
4. Mittaustulosten luominen
5. Mittaustuloksista tiedottaminen niitä tarvitseville vastuuhenkilöille

6. Mittaustulosten käyttäminen tietoturvallisuuden hallintajärjestelmän kehittämispäätöksissä
7. Mittaustulosten käyttö tietoturvallisuuden hallintajärjestelmän kehittämiskohteiden tunnistamisessa, mukaan lukien laajuus, käytännöt, tavoitteet, kontrollit, prosessit ja menettelytavat
8. Helpottaa tietoturvallisuuden mittausohjelman jatkuvaa parantamista (ISO/IEC 27004:2009, vi-vii).

4.1 Tietoturvallisuuden hallintajärjestelmän mittaamisen tavoitteet

Tietoturvallisuuden hallintajärjestelmän mittaamisen tavoitteita ovat seuraavat:

- Käyttöönotettujen kontrollien tai kontrolliryhmien toimivuuden arvioiminen
- Käyttöönotetun tietoturvallisuuden hallintajärjestelmän toimivuuden arvioiminen
- Tunnistettujen turvallisuusvaatimuksien saavuttamisen tarkistaminen
- Organisaation liiketoimintariskien hallinnan helpottaminen tuloksellisemmalla tietoturvallisuudella
- Materiaalin tuottaminen johdon katselmusta varten, helpottamaan tietoturvallisuuden hallintajärjestelmään kohdistuvaa päätöksentekoa sekä oikeuttamaan tarvittavat parannukset implementoituun järjestelmään (ISO/IEC 27004:2009, 4).

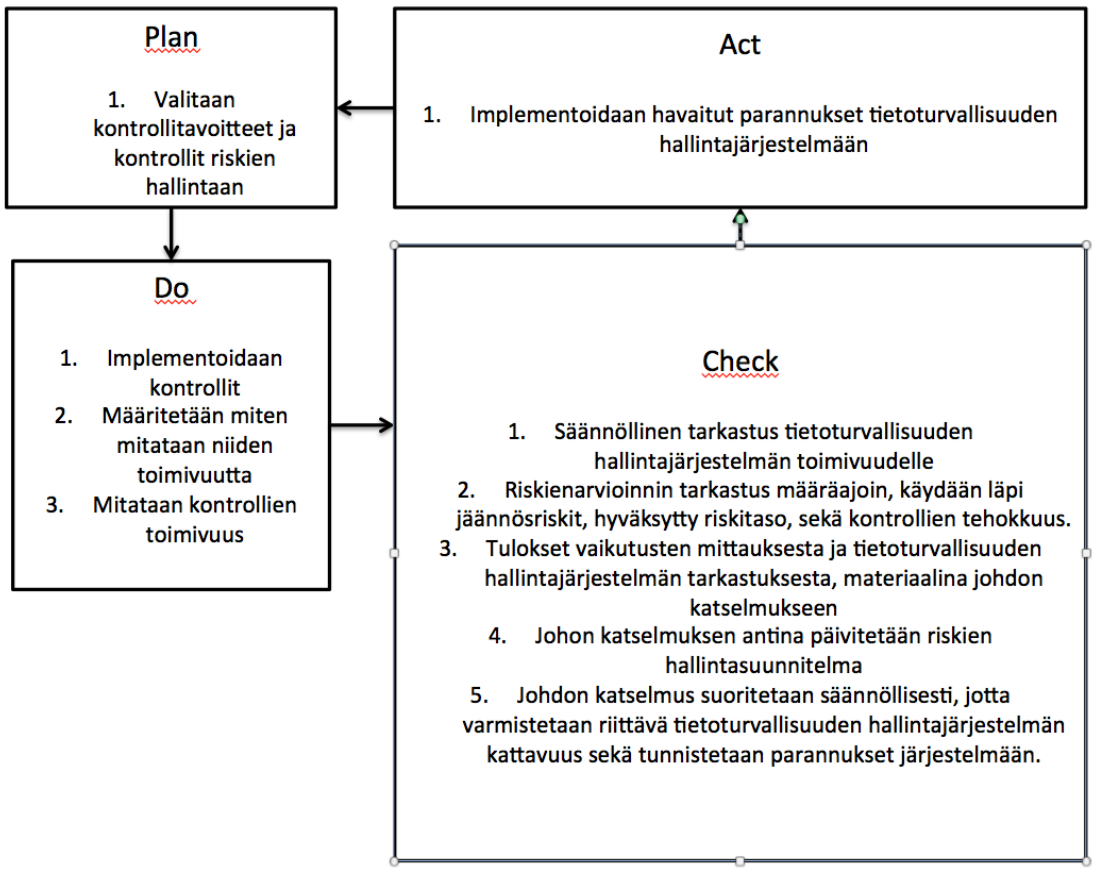
Tietoturvallisuuden hallintajärjestelmän mittaamisen tavoitteet kattavat koko organisaation tietotarpeet, kun mittaustuloksien analysointiin käytetään asiantuntijoita. Hyvin suoritettu mittaaminen ja sen tulosten tulkinta antaa organisaatiolle reaaliaikaisen ja todenmukaisen kuvan tietoturvallisuuden tilasta. Kaikki tämä on mahdollista ilman kallista ja laajaa hallintajärjestelmän auditointia.

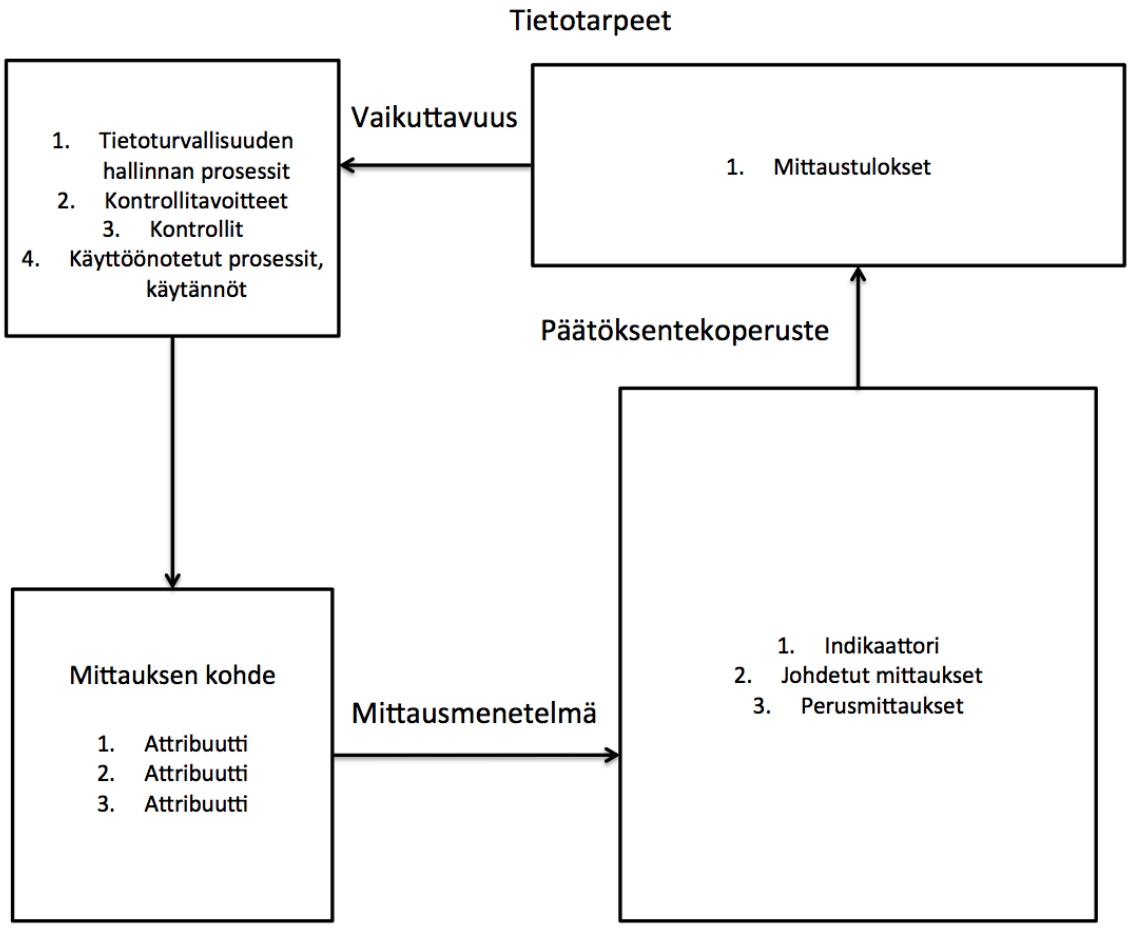
4.2 PDCA-malli

PDCA-malli tulee sanoista Plan, Do, Check ja Analyse/Act. PDCA-malli tarkoittaa jatkuvaa johtamisen prosessia ja keskeisiä menettelyitä, joilla tuetaan toiminnan suunnittelua, toteutusta, seurantaa ja toiminnan arviointia sekä johtopäätösten tekemistä. PDCA-malli on perustana johtamisen ja laadunhallinnan ISO 9000 -sarjan standardeissa sekä useissa muissa johtamisjärjestelmästandardeissa. (Biatec 2011.)

Käytän alla olevassa kuvassa PDCA-mallia tietoturvallisuuden hallintajärjestelmän mittariston kehittämiseen. Ensimmäisessä vaiheessa suunnitellaan mitä halutaan saavuttaa ja millä keinoin. Toisessa vaiheessa tehdään kontrollit ja varmistetaan ne toimiviksi. Kolmas vaihe sisältää koko organisaation laajuisen mittauksen tarkistamisen. Neljäs ja viimeinen vaihe on muutosten teko mittaristoon.

Kuvio 1. Tietoturvallisuuden mittaamisen PDCA-malli (Biatec 2011).





Kuvio 2. Tietoturvallisuuden mittausmalli. (ISO/IEC 27004:2009, 7).

Kuvio 2 kertoo tietoturvallisuuden mittaamisstandardin jatkuvan kehittämisen kierron.

Perusmittaus on yksinkertaisin mahdollinen mittaus. Perusmittaus muodostuu kun mittauksen kohteen attribuutteja eli ominaisuuksia mitataan mittausmenetelmän avulla. Mittausmenetelmällä voi olla monia attribuutteja, mutta vain muutama niistä tuottaa hyödyllisiä arvoja perusmittaukseen. Tiettyä attribuuttia voidaan käyttää useassa eri perusmittauksessa. Johdetut mittaukset kokoavat yhteen kaksi tai useampaa perusmittausta. Indikaattori on mittaus, joka tuottaa arvion tietyistä attribuuteista, jotka johdetaan analyyttisellä mallilla tietotarpeen rajoissa. (ISO/IEC 27004:2009, 7-10).

Havainnollistetaan kuviota esimerkillä tietoturvakoulutuksen mittaamisesta. Mittauksen kohde on henkilöstötietokanta. Sen attribuuttina on koulutusrekisteri.

Mittausmenetelmänä on koulutuksen saaneiden lukumäärän laskeminen tietokannasta. Perusmittauksista saadaan koulutukseen osallistuneiden lukumäärä ja sen suorittaneiden lukumäärä. Näistä lasketaan analyyttisellä mallilla koulutuksen edistyminen organisaatiossa. Indikaattori kertoo montako prosenttia käyttäjistä on koulutettu. Tämän jälkeen päätöksentekoperusteella luodaan mittaustulokset. Päätöksentekoperuste on seuraavanlainen: kun koulutuksen on läpäissyt 70% työntekijöistä niin, mittarin arvo on vihreä. 60% tarkoittaa keltaista; vähemmän kuin 60% punaista.

5 HAASTATTELUJEN TULOKSET JA ANALYYSI

Haastattelin kahdeksaa kaupungin tietoturvallisuuden hallintajärjestelmän avainhenkilöä vuonna 2010. Yhdeksäs avainhenkilö teki oman dokumenttinsa, jossa hän arvioi tietoturvallisuuden mittaamisen tilannetta oman toimipisteensä kannalta. Kävin kaikkien haastateltavien kanssa myös keskustelua kaupungin tietoturvallisuuden hallintajärjestelmän tilasta ja miten sen toimintaa tulisi kehittää ja seurata. Suurin yhteisymmärrys oli siitä, että järjestelmää täytyy mitata, muttei siitä saisi tulla resursseja kuluttavaa toimintaa. Koko hallintajärjestelmälle haluttiin yksinkertaista ja kevyttä rakennetta. Osa haastatelluista koki myös, etteivät he ole päivittäneet hallintajärjestelmän dokumentaatiota, koska eivät ymmärrä järjestelmän vaatimaa sanastoa tai toimintaa. He toivoivat järjestelmästä ymmärtävää henkilöä auttamaan ensimmäiselle päivityskerralle. On helpompi kirjoittaa kontrollien kohdalle ”ei tarkennuksia”, kuin ”en tiedä, mitä tässä tarkoitetaan”. Haastateltavat olivat yhtä mieltä siitä, että tietoturvallisuuden hallintajärjestelmä ilman ajantasaista dokumentaatiota ei toimi.

Haastattelulomake sisälsi 11 kysymystä sekä kohdan yleisiä huomioita, johon avainhenkilöillä oli mahdollisuus kertoa muita huomioita. Alla on kirjattu kysymykset. Jokaisen kysymyksen jälkeen analysoin niin vastauksia yleisesti kuin kysymyksiäkin. Työni vastaukset ovat luottamuksellisia ja ne jäävät salaisiksi.

Mitä teille tulee mieleen käsitteestä tietoturvallisuuden hallintajärjestelmän mittaaminen?

> Tulisi mitata tietoturvallisuuden eri osa-alueita vuosien saatossa. Henkilöstön osaaminen, virustorjunnat ja hyökkäykset, sekä tietoturvarikkomukset ja löytyykö niitä.
>
> Onko käsitteestä puhuttu? Järjestelmää ei mitata.
>
> Se tapa, jolla voidaan arvioida hallintajärjestelmän ja turvamekanismien vaikuttavuutta.
>
> Laadullinen selvitys. Tietyt tavoitteet ja kontrollit katsotaan mittaamisessa ja analysoidaan mitä, miksi ja miten.

Mittaamisen ongelma ja ajankäyttö. Mitä mittareiksi?

Ranking-lista intranettiin eri yksiköiden välillä.

Systeemi, jolla mitataan tietoturvahallintajärjestelmän toimintaa.

Monessa tilaisuudessa on arvioitu tietoturvallisuuden tilaa.

Kysymyksellä halusin avainhenkilöiden ensivaikutelman siitä, mitä käytössä olevan hallintajärjestelmän tuleva mittaaminen tuo mieleen. Vastauksien sisällöllinen hajonta on varsin suurta, aina hallintajärjestelmän laadusta ja kehityksestä mahdollisiin ongelmiin. Vastauksissa on myös viitteitä toiveista paremmuusjärjestykseen hallintokuntien sisällä ja selkeiden vastauksien antamiseksi niin hallintajärjestelmän tilasta kuin minne ollaan menossa. Hallintajärjestelmän ongelma on siinä, ettei sen perustaminen yksin riitä. Jollei vuosittain tapahdu edistystä, korjauksia ja parannuksia, erkanee dokumentoitu malli täysin kaupungin tietoturvallisuuden arjesta. Kenen vastuulla on vanhentuneesta dokumentaatiosta ja ohjeistuksesta aiheutuvat tietoturvahäiriöt?

Mitä mitattavia kohteita teille tulee mieleen?

Miten järjestelmät on suojattu ja ihmisten säännösten tuntemus.

Tietoturvan tiedostaminen on yksi mitattava kohde, sekä tiedon saanti ja kulku.

Palomuuri- ja virustorjuntahyökkäysten määrä, salasanakäytännöt ja kulunvalvonta.

Mitataan koulutuksen suorittamista ja osallistumista.

Jatkuvuus- ja toipumistoimenpiteet sekä säännönmukaiset tehtävät. Konkreettiset kehitysasiat ja niiden toteutuminen.

VAHTI-ohjeiden mukaisesti: hallinnollinen, henkilöstö-, fyysinen -, tietoaineisto-, tietoliikenne-, laitteisto-, ohjelmisto- ja käyttöturvallisuus.

Erilaiset tekniset kyselyt.

Toimiiko kaikki kuten kuuluu, tietoturvaskannaukset, verkonvalvonta.

Tietoturvallisuuden hallintajärjestelmän käyttöönotossa viimeisenä vaiheena valitaan vapaaehtoisista kontrolleista ne, joilla pyritään pienentämään ja hallitsemaan tietoturvariskejä. Periaatteessa jokaista kontrollia voitaisiin mitata ja

erotella, mitkä kontrollit edistävät tietoturvaa ja mitkä vain vaikuttivat hyviltä niitä valittaessa. Vastauksien valossa ihmisten tietoturvatietoisuus nousee tarkkailtavan mittauslistan kärkeen niin koulutukseen osallistumisessa kuin kysymyksien läpäisyssäkin. Kulunvalvonta lienee fyysisestä turvallisuudesta ilmeisin ja tärkein mitattava kohde. Myös hallintajärjestelmän kehittämisen ja säännönmukaisten tehtävien seuraaminen auttaa löytämään piileviä ongelmia. Lopuksi tulee mitata tietoturvahäiriöiden ja tapahtumien määrä niin verkkohyökkäyksien kuin saastuneiden työasemien normaalitilanteesta poikkeamisenkin osalta. Suuret vaihtelut suuntaan ja toiseen kielivät ongelmista.

Näkisittekö että tietoturvallisuuden mittaamisen tulisi olla kaupunkitasolla määriteltynä vai myös tarkennettuna hallintokuntien omilla lisäyksillä?

Pääosa kaupunkitasolla ja hallintokuntien lisäyksillä.

Ehdottomasti omilla lisäyksillä, toiminnot hyvin erilaisia.

Teknisessä mielessä pyritään yhtenäisyyteen, tarpeen mukaan hallintokuntien omilla lisäyksillä.

Määriteltynä kaupunkitasolla, hallintokuntakohtaisilla tarkennuksilla.

Kaupunkitasolla ydinperiaatteet, hallintokunnat omilla lisäyksillä.

Ei osaa sanoa.

Kaupunkitason perusmäärittely, hallintokunnille räätälöity.

Määriteltynä kaupunkitasolla ja myös hallintokuntakohtaisilla lisäyksillä. Mahdollisuus kevennettyyn määrittelyyn tulisi olla.

Kysymyksellä halusin tuoda esille, onko vahva keskitetty johtomalli paras vai tulisiko luoda suuntaviivat, joita hallintokunnat tarkentavat. Dokumentaation kannalta parasta olisi valmis formaatti, johon hallintokunnat eivät saa tehdä omia lisäyksiään. Tämä helpottaa tarkistamista sekä dokumentaatioiden vertaamista. Toisaalta, jos hallintokuntakohtaiset lisäykset vastaavat todenmukaista tilannetta paremmin ja dokumentaatio päivittyy ajallansa, on paikallinen räätälöinti tarpeellista. Vastauksien konsensus on, että pääpiirteet määritellään kaupunkitasolla ja hallintokunnat tekevät tarpeelliset tarkennukset.

Miten tärkeänä näette tietoturvallisuuden hallintajärjestelmän mittaamisen osion työnkuvanne kannalta?

Koskee nimityksen johdosta, ei ole ydinkysymys.

Tärkeänä.

Kuuluu työnkuvaan, kaupungin tietoturvaryhmä.

Tietoturvallisuus kuuluu riskien hallintaan, olennainen osa.

Voi liittyä tarkastusaiheeseen.

Näkee oman työnsä tulokset.

Työnkuvan varmistaa järjestelmän olemassaolo.

Kun tiedetään, mitä mitataan ja, miten voidaan pyrkiä tavoitteeseen. Vähemmän ihmettelyä. Mittaamalla voidaan todentaa oman toiminnan johdonmukaisuus kehityskohteisiin nähden.

Halusin kysyä, miten tietoturvallisuuden hallintajärjestelmän avainhenkilöt asennoituvat mahdolliseen tulevaan hallintajärjestelmän mittaamiseen, jossa heidän panoksena näkyy. Mittauksella toivotaan mahdollisimman todenmukaisia tuloksia, jotta tiedetään, mitä pitää parantaa, ja nähdään sen kautta minne pitää päästä. Esitän hypoteesin, että mitä toimivampi hallintajärjestelmä, sitä vähemmän sen ylläpidossa on työtä ja ongelmia.

Entäpä kaupungin X kannalta?

Järjestetty kriisitilanne ja miten seurataan miten siitä selvitty.

Olennaista. Hyvät käytänteet edistää välillisesti julkisuuskuvaa ja taloutta.

Tietoturvatasot sovellettuina Valtiohallinnon ohjeiden mukaan.

Erittäin tärkeänä. Laki vaatii tietoturvallisuutta. Täytyy mitata.

Hallintajärjestelmän asianmukaisuudesta ei voi varmistua kuin mittaamalla ja mittaamisen pohjalta tehtyjen päätösten kautta järjestelmää voidaan kehittää.

Aika tärkeänäkin. Ohjelmistojen ja koneiden päivitykset näistä käytettävyys. Testit kerran vuodessa.

Tietoturvaprojektit ovat olleet tasapainossa hallintokuntien ja keskusjohdon kanssa. Joko keskusjohto määrää miten hallintokunnat tekevät tai hallintokunnat määräävät itse. Liiallisen kirjavuuden estäminen on tärkeää.

Kaupungin kannalta halutaan toimivaa tapaa testata ja mitata, miten tietoturvallisuuden hallintajärjestelmä täyttää sille asetetut tavoitteet. Lisäksi halutaan mahdollisuutta puuttua ongelmiin jo niiden syntyvaiheessa, eikä vasta kun media revittelee etusivun uutisella.

Mitä pidätte hallintajärjestelmän mittaamisen toteuttamisen hyvinä puolina?

Tiedetään heikkoudet ja haavoittuvuudet sekä samalla saadaan koulutusta.

Järjestelmä konkretisoi vastuut, sekä saadaan standardoitua vertailukelpoista aikasarjaa.

Nähdään ollaanko menossa oikeaan suuntaan hallintajärjestelmässä. Keskittyykö oikeisiin asioihin.

Täytyy tietää nykytilanne, jotta nähdään kehityskohteet.

Mittaamisen kautta järjestelmää voidaan kehittää. Tietoturvallisuuden merkitys on korostunut. Valvonta ja seuranta on osa johtamista ja hallintaa.

Nähdään muutos toistettaessa mittaukset.

Yhtenäistyminen ja sitä kautta yhteismitallisuus. Voidaan vertailla läpi kaupungin hallintokuntien.

Objektiivisen tiedon, vertailukelpoisuuden tarve. Haasteena miten tehdään ihmisille mieluinen vastata ja ymmärrettävä tulos.

Mittaamisen hyvinä puolina vastauksista huokuu kehitys ja toistuvien mittausten tuoma objektiivisuus sekä tilannekuva nyt ja huomenna.

Entä hallintajärjestelmän mittaamisen toteuttamisen huonoina puolina?

Ei liikaa mittaamista. Sen tulisi olla osa kokonaisuutta. Sähköiset kaavakkeet tulisi olla kerralla silmäiltävissä, eikä kompakysymyksiä.

Varautunut asenne ja mahdolliset toteutusongelmat.

Työmäärät lisääntyvät ja järjestelmän tulee toimia.

Voi aiheuttaa negatiivista ja väärää palautetta. Mittaamisen tulisi olla rakentavaa. Ei voi arvostella kuin matematiikan koetta.

Mittarit alkavat ohjata toimintaa. Trendien seuranta.

Suositukset ja parannusehdotukset voidaan kokea arvosteluna ja kustannuksina.

Tulisi olla järkevät mittarit, jotka kuvaavat tilannetta oikein.

Aikaa ja resursseja kuluu. Kustannuksien ja riskien tasapaino tärkeää.

Mittaamisen varjopuoliin kuuluu selvästi mahdollinen työmäärän lisääntyminen, ja puutteelliset resurssit. Sekä se, että jos mittareihin voi vaikuttaa liian helposti, tehdään vain se, mitä mittaristo vaatii. Myös mittaamisen ja mittaustulosten tulkitsijan objektiivisuus herättää kysymyksiä. Ideaalitilanteessa mittariston laatija ja tulosten tulkitsija ovat eri henkilöt.

Onko teillä käytössä jo hallintajärjestelmän toimivuuden tai soveltamissuunnitelman mukaisia mittareita?

Koulutus ja riskien arviointi, sekä palveluntarjoajien laatupalaverit.

Johdonkatselmuksessa on katsottu onko tehty mitä pitää ja ollaanko aikataulussa.

Ei tietääkseni.

Säännönmukaiset tehtävät, koska viimeksi tehty. Aikataulu-mittarit.

Laatupalaverit, virustorjunnat, palvelimien käytettävyysprosentit ja tietoverkkojen katkokset.

Käsittääkseni ei ole.

Ei ole käytössä mittareita. Miten henkilökunta on käynyt tietoturvakoulutuksessa.

Hallintokunnissa ei vielä mitata hallintajärjestelmän toimivuutta muutamaa poikkeustapausta lukuun ottamatta. Useassa kohteessa asiaa on sentään pohdittu joko johdon katselmuksessa tai säännönmukaisten tehtävien aikataulujen kautta.

Tuleeko mieleenne mitattavia kohteita, joissa on organisaation tietoturvatavoitteiden kannalta parannettavaa?

Järjestelmä pyörimään ja työrauha.

Salasanan vanheneminen ei ole kaikissa järjestelmissä.

Kenelle järjestelmästä tulisi raportoida? Tietoturvan kehittämiseen yhteistyötä läpi hallintokuntien aina keskushallintoon saakka.

Koko kaupungille, se mitä jo muissa hallintokunnissa seurataan.

Kaikkien mitattavien kohteiden osalta on parannettavaa jotta voidaan varmistaa tietoturvallisuuden asianmukaisuus.

Korvienväli.

Henkilöstöturvallisuus.

Tietoturvallisuuden avainhenkilöiden mietteet mitattavista kohdista eriävät suuresti toisistaan. Näen suurimpana toiveena yhdenmukaisen mittaustavan ja mittariston. Myös järjestelmän aiheuttamien mittaustulosten raportointi aiheuttaa kysymyksiä. Paras ratkaisu olisi, että joka hallintokunnan oma tietoturvavastaava raportoisi keskitetysti koko kaupungin tietoturvavastaavalle. Näistä kootaan yhteinen tietoturvallisuuden hallintajärjestelmän toiminnan ja kehittämisen raportti johdon katselmukseen.

Tulisiko mahdollisen mittaustavan mielestänne perustua mieluiten:

1. Mittaamisen standardiin ISO/IEC 27004:2009?
2. Valtiovarainministeriön ICT-varautumisen mukaisiin mittausperiaatteisiin?
3. Velvoittavaan lainsäädäntöön?
4. Johonkin muuhun tapaan?

Sama mikä, kunhan on hyvä. Riittävästi muttei liikaa.

Ei osaa sanoa.

Valtiovarainministeriön ICT-varautumisen mukaisiin mittausperiaatteisiin.

2, toisena 1, ei mieluusti lakia.

2, koska luotu Suomen oloihin ja julkishallintoon.

2.

2, Suomen oloihin.

Velvoittava lainsäädäntö ensisijaisesti, toisena standardi, kolmantena listalla laki ja jokin muu tapa.

Haastateltavat ovat liki yhtä mieltä siitä, että mittauksen tulisi perustua Suomen tarpeiden mukaiseen ICT-varautumisen mittausperiaatteisiin. Ikävä kyllä ICT-varautumisen mittaustavat ovat tällä hetkellä salaisia ja todennäköisesti valtiovarainministeriön alaisuudessa. Uskon, että paras tapa mitata on aloittaa kevyellä mittarilla, joka kasvaa kattamaan organisaation tarpeet PDCA-mallin mukaisesti.

Millä tavalla tulisi mielestänne kerätä kehittämisehdotukset tietoturvallisuuden mittaamisesta, jotta saataisiin mielipiteet johdolta, asiantuntijoilta ja työntekijöiltä?

Johtoryhmät ja IT-johtoryhmä.

Kysely hallintokunnan johtajalle.

Verkoston kautta tiedonkulku asiantuntijoilta ja työntekijöiltä. Johdon tulee luottaa asiantuntijoihin.

Kvantitatiivinen kysely, vapaa sana osiolla.

Henkilökohtaiset haastattelut ja otos henkilökunnasta.

Sähköinen kysely ja haastattelu tai työpaja.

Raportti ylimmälle johdolle, asiantuntijat 4 krt vuodessa tapaaminen, työntekijöille koulutus.

Aika ajoin palaute ja keskustelut.

Haastateltavat haluavat kyselyn, haastattelun tai tapaamisen tapoina, joilla parantaa tietoturvallisuuden hallintajärjestelmän mittaamista. Pidän toimivampana tapana sellaista, joka tuo jatkuvuutta säännöllisin sovituin väliajoin. Hallintokuntien tietoturvallisuuden avainhenkilöiden tulisi kokoontua 4 kertaa vuodessa ja käydä läpi mittaamisen tuloksia. Tulokset sisältävät myös työntekijöiden tietoturvakoulutuksen mittausta sekä palautetta mittausjärjestelmästä. Tästä kaikesta luodaan raportti ylimmälle johdolle. Raportti sisältää toimenpide-ehdotukset, huomioitavat poikkeamat ja yleiskuvan organisaation tietoturvan tilasta.

Yleisiä huomioita:

Resurssit.

Johdon tuki.

Varautumiskyselyt.

Ei kannata mittareilla, jos niihin ei voi vaikuttaa.

Tietoturvalaatikko sähköpostiin.

Kaikki yleiset huomiot ovat tärkeitä. Havainto resurssien riittämisestä, jos hallintokunnalla tietoturvallisuutta hoitava henkilö tekee myös muita töitä. Johdon tuki aiheuttaa kysymyksiä, sillä kaikki mikä kuluttaa aikaa ja rahaa, tulee perustella huolella, ja huolellisia perusteluja saadaan vasta, kun mittaamalla saavutetaan tuloksia.

Yksi haastateltava on sitä mieltä, ettei kannata mitata, jos mittareihin ei voi vaikuttaa. Tämä on koko mittariston kannalta elintärkeä huomio. Johdon tulee antaa resurssit ja valta vaikuttaa mittaamisen tuloksena löytyneisiin poikkeamiin. Lopuksi tietoturvalaatikko sähköpostiin helpottaisi tavallisen työntekijän mahdollisuutta ilmoittaa tietoturvapoikkeamista. Poikkeamasta ilmoittamisesta tulisi vielä lisäksi palkita, jotta asian tärkeys on kaikille selvä.

6 TIETOTURVAN MITTAAMISEN TOTEUTTAMISEHDOTUKSET - YHTEENVETO

Aloittaessani kaupungin tietoturvallisuuden hallintajärjestelmän mittariston selvittämisen sain varhaisessa vaiheessa toiveen portaittaisesta mittaristosta. Mittaristo tulisi saada ensimmäisessä käyttöönottovaiheessaan mahdollisimman helposti läpi koko kaupungin organisaation. Joten ensimmäinen ehdotukseni mittaristoksi on kuuden mittarin mittaristo, jonka tuloksia luetaan liikennevalojen värikoodein: vihreä tarkoittaa kaikki on kunnossa, keltainen että tilannetta pitää seurata ja punainen välitöntä puuttumista ongelmaan. Mittariston luontevimmaksi paikaksi olen pohtinut ServiceDeskiä. Sen kauttaa kulkee pääosa koko kaupungin IT-ongelmatilanteista, mutta toisaalta siitä syystä heitä ei halua kohtuuttomasti kuormittaa ajoittaisilla mittauksilla ja kaavioiden kirjaamisella.

Ensimmäiseksi mittariksi ajattelin itse tietoturvallisuuden hallintajärjestelmän säännönmukaisten tehtävien ajallaan tapahtuvaa mittausta. Tämä siitä syystä, että jos hallintajärjestelmän toiminnat ovat jäljessä aikataulustaan, suurella todennäköisyydellä eivät niiden kontrolloimat riskit ole hallinnassa. Tietoa kerätään neljän kuukauden välein tai tiheämmin, jos hallintajärjestelmän avainhenkilöt niin päättävät. Tämä mittari on parhaiten toteutettavissa yhteisellä kokouksella, jossa ovat paikalla kaikki hallintokuntien tietoturvavastaavat ja he käyvät yhdessä läpi tilannetta ja mahdollisia ongelmakohtia. Tämän kokouksen tulokset kirjataan mittariin.

Toinen mittari olisi henkilökunnan koulutus. Se jaetaan tietoturvahenkilökunnan ja muun henkilökunnan välillä kahdeksi mittaristoksi. Jokaisen tietoturva- tai työkoulutuksen jälkeen tulisi mahdollisuuksien mukaan tehdä lyhyt A4-mittainen testi koulutuksesta ja tallentaa testin tulokset seuraavasti: 70% testistä oikein, mittarin arvo vihreä, 60% keltainen ja alle 60% punainen. Tosin arvot ovat vain viitteelliset ja niitä tulee suhteuttaa tarpeen vaatiessa, jotta ne kuvaavat, onko

koulutuksesta saatu se, mitä siltä haluttiin. Mahdollinen seurantakysely tehtäisiin myöhemmin.

Kolmas mittari olisi kulunvalvonta. Sen ongelmia tulisi voida raportoida kevyesti ennen kuin on tarpeen kutsua virkavaltaa paikalle mahdollisten kutsumattomien vieraiden vuoksi. Periaate on yksinkertainen: Ne tilat ja ovet, joissa on jokin pääsyn estävä mekanismi (kulkukortti, avain, tai muu vastaava) ovat eijulkisia tiloja. Jos kokous tai vastaava vaatii jättämään oven auki, asia tulee kirjata ja siihen tulee puuttua. Fyysisen turvallisuuden tarpeellisuutta ei tule vähätellä.

Neljäs mittari on dataa, joka saadaan suoraan ServiceDeskistä, eli haittaohjelmatartuntojen määrä, moniko niistä aiheutti ongelmia ja miten monta haittaohjelmaa löytyi. Samassa mittarissa tulisi olla myös verkkohyökkäyksien dataa. Onko palvelunestohyökkäyksiä, onko töhritty julkisia sivua, tai onko yritetty tunkeutua potilastietokantoihin. Koska internetissä on jatkuva vanhojen haittaohjelmien ja porttiskannereiden tulva, myös poikkeamat tästä “taustasäteilystä” tulee kirjata.

Viidentenä mittarina ehdottaisin käytettävyysmittaria. Tämä sisältää dataa siitä, mitkä ongelmat ovat aiheuttaneet toiminnan häiriöitä ja miten pitkäksi aikaa. On kyseessä sitten Intranetin keskustelupalsta tai varmuuskopiotiedostot palvelimella, kaikki katkokset ja normaalitilasta poikkeavuudet kartuttavat käytettävyysmittaria. Tämä kertoo myös, miten hyvin käyttäjät pääsevät raportoimaan ongelmistaan ja kauanko niiden selvittämisessä menee.

Kuudentena mittarina pitäisin tietoturvapäivitysten testaamisen ja asentamisen seurantaa. Paljonko aikaa kuluu siitä, kun ohjelmistonvalmistaja julkaisee korjaavan ohjelmistopäivityksen, kunnes se on asennettu läpi koko organisaation. Seurantaan tulee myös kirjata, mitä ongelmia ilmenee, ja näin täydentää mittarin mitattavien kohteiden listaa.

7 POHDINTA

Tietoturvallisuuden hallintajärjestelmän mittaamisen kartoitus on ollut palkitseva kokemus. Tietoturvallisuuden mittaaminen on erittäin haastavaa, eikä maailmanlaajuisesti ole löydetty vielä parasta tapaa mitata. Tietoturvallisuuden mittaamisstandardin mukainen mittaristo on liian työläs ja pikkutarkka. Se sopii hyvin teoreettiseksi viiteaineistoksi, ei normaalille organisaatiolle mittaristoksi. Valtiovarainministeriön tietoturvatasot- ja ICT-varautuminen hankkeiden on tarkoitus sisältää myös mittaaminen. Nämä resurssit on poistettu valtiovarainministeriön sivuilta. Tietääkseni ICT-varautuminen ja tietoturvatasot ovat yhä olemassa, mutta ne ovat nyt salaisia.

Tutkiessani erilaisia tapoja mitata tietoturvallisuutta huomasin varsin suuren määrän yliampuvia mittaristoja. Mittaristo saattaa sisältää satoja mitattavia kohteita, ja mittaustulosten aiheuttama dokumentaatio on useita kymmeniä sivuja. Nämä tietoturvallisuuden mittarit ovat käytännöllisiä vasta tietoturvallisuuden hallintajärjestelmän mittaamisen auditoinnissa ja vaativat valtavat määrät resursseja.

Uskon, että paras tapa luoda toimiva tietoturvallisuuden hallintajärjestelmän mittaristo on aloittaa vain muutamalla mitattavalla kohteella ja lisätä mitattavia kohteita organisaation mittausten perusteella. Tietoturvallisuuden avainhenkilöiden tulee vahvistaa organisaation tietoturvan nykytilaa, sen heikoimmasta kohdasta, ja tehdä yhteistyötä läpi koko organisaation yhteistyöverkon, johon kuuluvat niin toimistotyöntekijät, alihankkijat, johtoryhmä kuin tietoturva-auditoijakin.

Tietoturvallisuuden mittaamisen ei tulisi olla leimaavaa ja poliisimaista kuulustelua, vaan opettavaa ja ohjaavaa asioiden korjaamista, jonka tavoitteena on välttää aiemmin tehtyjen virheiden toistaminen. Tietoturvallisuus toimii vain yhteistyöllä, eikä ulkokultaisilla auditoinneilla, jotka eivät näe koko totuutta. Auditoijat

jäävät helposti organisaation luoman tietoturvadokumentaation vangeiksi käytännön toimien tarkastamisen sijaan.

Tulevaisuudessa tietoturvallisuuden mittaamisongelmaa ratkaistaessa tulisi keskittyä toiminnallisuuteen ja helppoon käyttöönottoon. Mittaustapoja tulee aina lisää, mutta toimiva mittausjärjestelmä vaatii muutaman järjestelmää hoitavan osaavan työpanoksen sekä johdon vahvan osallistumisen. Pahinta on antaa mittausdokumentaation ja todellisten arkipäivän tietoturvapoikkeamien olla ristiriidassa.

LÄHTEET

Anonymous; Balding, C. & Kajala, T. 2002. Hakkerin käsikirja. Edita.

Biatec Oy. 2008. PDCA-malli. Viitattu 30.10.2011 http://www.biatec.fi/PDCA-malli.html.

Boyens, J.; Paulsen, C.; Moorthy, R. & Bartol, N. 2014. Supply Chain Risk Management Practices for Federal Information Systems and Organizations. NIST Special Publication 800-161. Second Public Draft. Viitattu 11.6.2014. http://insidecybersecurity.com/iwpfile.html?file=jun2014%2Fcs06042014_NIST_Supply_Chain.pdf.

ENISA 2014. About ENISA. Viitattu 9.6.2014. http://www.enisa.europa.eu/about-enisa.

Hayden, L. 2010. IT Security Metrics. The McGraw-Hill Companies, Inc.

ISO/IEC 27004:2009. Information technology - Security techniques - Information security management - Measurement.

ISO/IEC 27003:2010. Information technology - Security techniques - Information security management system implementation guidance.

Pagett, J. & Ng, S. 2010. Risk Metrics: Measuring the effectiveness of an IT security control. Viitattu 5.6.2014. http://www.computerweekly.com/feature/Risk-metrics-Measuring-the-effectiveness-of-an-IT-security-control.

Ross, R; Oren, J. & McEvilley, M. 2014. Systems Security Engineering. NIST Special Publication 800-160. Initial Public Draft. Viitattu 9.6.2014. http://csrc.nist.gov/publications/drafts/800-160/sp800_160_draft.pdf.

Swift, D. 2006. A Practical Application of SIM/SEM/SIEM Automating threat identification. Viitattu 5.6.2014. http://www.sans.org/reading-room/whitepapers/logging/practical-application-sim-sem-siem-automating-threat-identification-1781.

Valtiovarainministeriö 2011. Kuntien ICT-varautuminen esitutkimus. Viitattu 5.6.2014. http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/03_kunnat/20110118Kuntie/Kuntien_ICT-varautuminen.pdf.